

EXPLICIT p -ADIC UNIT-ROOT FORMULAS FOR HYPERSURFACES

MASHA VLASENKO

ABSTRACT. We prove a statement on p -adic continuity of matrices of coefficients of the logarithm of the Artin-Mazur formal group law associated to the middle cohomology of a hypersurface. As J. Stienstra discovered in 1986, the entries of these matrices are coefficients of powers of the equation of the hypersurface, and in certain cases they satisfy congruences of Atkin and Swinnerton-Dyer type. These congruences imply that eigenvalues of our limiting matrices are eigenvalues of Frobenius of zero p -adic valuation on the middle crystalline cohomology of the fibre at p .

CONTENTS

| | |
|--|---|
| 1. p -adic continuity of Stienstra's matrices | 1 |
| 2. Main lemma on congruences for the powers of $\Lambda(x)$ | 2 |
| 3. Proof of Theorem 1 | 4 |
| 4. The case of a smooth projective hypersurface | 5 |
| 5. Application of Atkin and Swinnerton-Dyer type congruences | 6 |
| 6. An example | 7 |
| References | 8 |

This note was written in preparation for the talk given at Max Plank Institute for Mathematics in Bonn on the 14th of January 2015. The author is grateful to Jan Stienstra for helpful conversations on the subject a while ago, in Bonn and Utrecht. Our main result is on the p -adic continuity, which was suggested by him in [2, p.1114].

1. p -ADIC CONTINUITY OF STIENSTRA'S MATRICES

Let R be a commutative ring and $\Lambda \in R[x_1^{\pm 1}, \dots, x_N^{\pm 1}]$ be a Laurent polynomial in N variables, which we will write as

$$\Lambda(x) = \sum_u a_u x^u, \quad a_u \in R,$$

where the summation runs over a finite set of vectors $u = (u_1, \dots, u_N) \in \mathbb{Z}^N$ and x^u means $x_1^{u_1} \dots x_N^{u_N}$. The *support* of Λ is the set of exponents of monomials in Λ , which we denote by $\text{supp}(\Lambda) = \{u : a_u \neq 0\}$. The *Newton polytope* $\text{Newt}(\Lambda) \subset \mathbb{R}^N$ is the convex hull of $\text{supp}(\Lambda)$.

Consider the set of internal integral points $J = \text{Newt}(\Lambda)^\circ \cap \mathbb{Z}^N$, where $\text{Newt}(\Lambda)^\circ$ denotes the topological interior of the Newton polytope. If $\text{Newt}(\Lambda)$ belongs to a hyperplane, we restrict to that hyperplane to define $\text{Newt}(\Lambda)^\circ$. Let $h = \#J$ be the number of internal integral points in the Newton polytope. Consider the following sequence of $h \times h$ matrices $\{\beta_n; n \geq 0\}$ with entries in R whose rows and columns are indexed by the elements of J :

$$(1.1) \quad (\beta_n)_{u,v \in J} = \text{the coefficient of } x^{(n+1)v-u} \text{ in } \Lambda(x)^n.$$

Let p be a prime number. Assume that R is endowed with a p th-power Frobenius endomorphism, that is a ring endomorphism $\Phi : R \rightarrow R$ satisfying

$$(1.2) \quad \Phi(r) \equiv r^p \pmod{p}, \quad r \in R.$$

Below we apply Φ to $h \times h$ matrices with entries in R entry-wise. This is an endomorphism of the ring of matrices but not a p th-power Frobenius: property like (1.2) won't be satisfied in general for matrices of size $h > 1$. We restrict our attention to the sub-sequence $\alpha_s := \beta_{p^s-1}$, $s \geq 0$. The entries of these matrices are then given by

$$(\alpha_s)_{u,v \in J} = \text{the coefficient of } x^{p^s v - u} \text{ in } \Lambda(x)^{p^s - 1}.$$

Date: January 20, 2015.

Theorem 1. (i) For every $s \geq 1$

$$\alpha_s \equiv \alpha_1 \cdot \Phi(\alpha_1) \cdot \dots \cdot \Phi^{s-1}(\alpha_1) \pmod{p}.$$

(ii) Assume that all matrices α_s are invertible. Then for every $s \geq 1$

$$\alpha_{s+1} \cdot \Phi(\alpha_s)^{-1} \equiv \alpha_s \cdot \Phi(\alpha_{s-1})^{-1} \pmod{p^s}.$$

The proof of this theorem will be given in the next two sections. It is unessential that we multiply by the inverse matrices on the right in (ii). The same congruence is true if one multiplies on the left, which is clear from the proof given in Section 3:

$$\Phi(\alpha_s)^{-1} \cdot \alpha_{s+1} \equiv \Phi(\alpha_{s-1})^{-1} \cdot \alpha_s \pmod{p^s}.$$

Therefore we have two p -adic limits

$$(1.3) \quad \alpha = \lim_{s \rightarrow \infty} \alpha_s \cdot \Phi(\alpha_{s-1})^{-1}, \quad \alpha' = \lim_{s \rightarrow \infty} \Phi(\alpha_{s-1})^{-1} \cdot \alpha_s,$$

but characteristic polynomials of the two $h \times h$ matrices α and α' are clearly the same.

It seems that matrices (1.1) first appeared in [1, 2] in the relation to the hypersurface X given by the equation $\Lambda(x) = 0$. Namely, it is shown in [1, Theorem 1] that (under the conditions that R is Noetherian and X is a projective hypersurface of degree $d > N$, flat over R) the Artin-Mazur functor $H^{N-1}(X, G_{m,X}^\wedge)$ is a formal group over R of dimension $h = \binom{d-1}{N}$. If in addition R is flat over \mathbb{Z} , the logarithm of this formal group law is given by

$$\ell(\tau) = \sum_{m=1}^{\infty} \frac{\beta_{m-1}}{m} \tau^m.$$

More precisely, the logarithm is the h -tuple of power series $\{\ell_u(\tau); u \in J\}$ in h -tuple of variables $\{\tau_u; u \in J\}$ given by $\ell_u(\tau) = \sum_{m=1}^{\infty} \frac{1}{m} \sum_{v \in J} (\beta_{m-1})_{u,v} \tau_v^m$. In [2] another congruences for matrices $\{\beta_n; n \geq 0\}$ were proved in the case when X is a double covering of \mathbb{P}^n and R is flat over \mathbb{Z} . These latter congruences generalize those of Atkin and Swinnerton-Dyer for elliptic curves. We discuss them in Section 5 and derive the consequences for the limiting matrices (1.3), which will explain the title of this paper. In [2, p.1115] Jan Stienstra mentions that congruences of Atkin and Swinnerton-Dyer type can be proved for complete intersections using a similar method. This would mean that in a rather general setting eigenvalues of the limiting matrices (1.3) are eigenvalues of the Frobenius operator acting on the middle crystalline cohomology of the fibre of X at p .

Matrix $\alpha_1 = \beta_{p-1}$ appeared earlier in [3]: for a smooth projective hypersurface X , α_1 modulo p is the matrix of the Cartier operator in a certain basis $\{w_u; u \in J\}$ of $H^0(\overline{X}; \Omega_{\overline{X}/\mathbb{F}_p}^{N-1})$. The details are given in Section 4.

It seems that congruences similar to those of Theorem 1 were considered in [4]. However, our statement is explicit and for the moment we will not investigate this possible relation.

2. MAIN LEMMA ON CONGRUENCES FOR THE POWERS OF $\Lambda(x)$

The ideas in this section are due to Anton Mellit and were introduced in [5]. We reproduce them here for the sake of completeness, and also because we need a formulation with Frobenius.

We extend the Frobenius morphism $\Phi : R \rightarrow R$ to the ring of Laurent polynomials $R[x_1^{\pm 1}, \dots, x_N^{\pm 1}]$ by setting $\Phi(x_i) = x_i^p$, so that

$$\Phi\left(\sum_u a_u x^u\right) = \sum_u \Phi(a_u) x^{pu}.$$

It is again a p th-power Frobenius morphism of the ring of Laurent polynomials: $\Phi(\Gamma) \equiv \Gamma^p \pmod{p}$ for any Laurent polynomial $\Gamma(x)$.

For a non-negative integer n , let $\ell(n)$ be the length of the expansion of n to the base p :

$$n = n^{(0)} + n^{(1)} p + n^{(2)} p^2 + \dots + n^{(\ell(n)-1)} p^{\ell(n)-1}, \quad 0 \leq n^{(i)} \leq p-1.$$

For two integers $n_1, n_2 \geq 0$ we denote by

$$n_1 * n_2 := n_1 + p^{\ell(n_1)} n_2$$

the integer whose expansion to the base p is the concatenation of the respective expansions of n_1 and n_2 .

With a Laurent polynomial $\Lambda(x)$ we associate a sequence of Laurent polynomials $\{I_{\Lambda,n}(x); n \geq 0\}$ uniquely defined by the condition that for every $n \geq 0$

$$(2.1) \quad \Lambda^n = \sum_{n_1 * \dots * n_r = n} I_{\Lambda,n_1} \cdot \Phi^{\ell(n_1)}(I_{\Lambda,n_2}) \cdot \Phi^{\ell(n_1) + \ell(n_2)}(I_{\Lambda,n_3}) \cdot \dots \cdot \Phi^{\sum_{j=1}^{r-1} \ell(n_j)}(I_{\Lambda,n_r}).$$

The summation here runs over all possible tuples of non-negative integers whose expansions to the base p concatenate to the expansion of n , so the number of parts r varies between 1 and $\ell(n)$. For every n the right-hand side consists of the term $I_{\Lambda,n}$ plus the sum of products of various $I_{\Lambda,n'}$ with $n' < n$ and their images under powers of Frobenius. Therefore this formula defines all $I_{\Lambda,n}$ recursively.

Lemma 1. *Polynomials $\{I_{\Lambda,n}; n \geq 0\}$ enjoy the following properties:*

- (i) $\text{Newt}(I_{\Lambda,n}) \subseteq n \text{ Newt}(\Lambda)$;
- (ii) $I_{\Lambda,n} \equiv 0 \pmod{p^{\ell(n)-1}}$.

Proof. Part (i) easily follows by induction. To prove (ii) an alternative construction of the polynomials $I_{\Lambda,n}$ can be given, in which the congruence becomes apparent.

For a Laurent polynomial $\Gamma(x)$ define a sequence of Laurent polynomials $\{R_s(\Gamma); s \geq 0\}$ by

$$R_s(\Gamma) := \Gamma^{p^s} - \Phi(\Gamma)^{p^{s-1}}$$

when $s \geq 1$ and $R_0(\Gamma) := \Gamma$. These polynomials were called *ghost terms* of Γ in [5]. The following properties of ghost terms easily follow by induction on $s \geq 0$:

- $\Lambda(x)^{p^s} = R_0(\Phi^s(\Lambda)) + R_1(\Phi^{s-1}(\Lambda)) + \dots + R_{s-1}(\Phi(\Lambda)) + R_s(\Lambda)$;
- $R_s(\Lambda) \equiv 0 \pmod{p^s}$;
- $\text{Newt}(R_s(\Lambda)) \subseteq p^s \text{ Newt}(\Lambda)$.

Expanding an integer n to the base p as $n = n^{(0)} + n^{(1)}p + n^{(2)}p^2 + \dots + n^{(\ell(n)-1)}p^{\ell(n)-1}$ with digits $0 \leq n^{(i)} \leq p-1$ we use the first property of ghost terms to decompose the product

$$\Lambda^n = \Lambda^{n_0}(\Lambda^{n_1})^p \dots (\Lambda^{n_{\ell(n)-1}})^{p^{\ell(n)-1}}$$

as the sum of products of ghost terms of images under powers of Φ of the collection of p Laurent polynomials Λ^a , $0 \leq a \leq p-1$. We obtain that

$$\Lambda^n = \sum_{\substack{m = (m_0, m_1, \dots, m_{\ell(n)-1}) \\ 0 \leq m_i \leq i}} R_m(n, \Lambda)$$

where

$$R_m(n, \Lambda) := \prod_{i=0}^{\ell(n)-1} R_{m_i}(\Phi^{i-m_i}(\Lambda^{n^{(i)}}))$$

and the summation above runs over the set of all integral tuples $m = (m_0, m_1, \dots, m_{\ell(n)-1})$ of length $\ell(n)$ satisfying $0 \leq m_i \leq i$. For such a tuple we denote $|m| = \sum_i m_i$. The second and third properties of ghost terms yield respectively

- $R_m(n, \Lambda) \equiv 0 \pmod{p^{|m|}}$;
- $\text{Newt}(R_m(n, \Lambda)) \subseteq n \text{ Newt}(\Lambda)$.

We consider the operation of concatenation on tuples

$$(m_0, \dots, m_{k-1}) * (m'_0, \dots, m'_{s-1}) := (m_0, \dots, m_{k-1}, m'_0, \dots, m'_{s-1}).$$

A tuple m satisfying $0 \leq m_i \leq i$ is called *indecomposable* if it can not be written as a concatenation of two shorter tuples with the same property. If m is an indecomposable tuple of length k then $|m| \geq k-1$, which can be proved by induction in k . For each $n \geq 0$ consider the Laurent polynomial

$$J_{\Lambda,n} := \sum_{\substack{m \text{ indecomposable} \\ \text{of length } \ell(n)}} R_m(n, \Lambda).$$

It is clear that $J_{\Lambda,n} \equiv 0 \pmod{p^{\ell(n)-1}}$ because $R_m(n, \Lambda) \equiv 0 \pmod{p^{\ell(n)-1}}$ for every indecomposable tuple m of length $\ell(n)$.

Every tuple m of length $\ell(n)$ can be uniquely written as a concatenation of indecomposable tuples $m = m_1 * \dots * m_r$ for some $1 \leq r \leq \ell(n)$, and if we chop the expansion of n to the base p into r blocks of respective lengths, $n = n_1 * \dots * n_r$, we then have

$$R_m(n, \Lambda) = R_{m_1}(n_1, \Lambda) \cdot \Phi^{\ell(n_1)}(R_{m_2}(n_2, \Lambda)) \cdot \Phi^{\ell(n_1) + \ell(n_2)}(R_{m_3}(n_3, \Lambda)) \cdot \dots \cdot \Phi^{\sum_{j=1}^{r-1} \ell(n_j)}(R_{m_r}(n_r, \Lambda)).$$

Here n_i 's are blocks of p -adic digits rather than integers, but the notation clearly extends to this case. Suppose n_i is a block of digits of length $\ell(n_i) > 1$ with the right-most digit being a zero. Since the tuple m_i is indecomposable, its right-most number is greater than 0. This implies $R_{m_i}(n_i, \Lambda) = 0$ because all higher ghost terms of the constant polynomial $\Lambda^0 = 1$ vanish. It follows that

$$\begin{aligned} \Lambda^n &= \sum_{\substack{\text{all tuples } m \\ \text{of length } \ell(n)}} R_m(n, \Lambda) \\ &= \sum_{n_1 * \dots * n_r = n} J_{\Lambda, n_1} \cdot \Phi^{\ell(n_1)}(J_{\Lambda, n_2}) \cdot \Phi^{\ell(n_1) + \ell(n_2)}(J_{\Lambda, n_3}) \cdot \dots \cdot \Phi^{\sum_{j=1}^{r-1} \ell(n_j)}(J_{\Lambda, n_r}), \end{aligned}$$

where in the upper sum tuples $m = (m_0, \dots, m_{\ell(n)-1})$ are assumed to satisfy the usual condition $0 \leq m_i \leq i$ for all $0 \leq i \leq \ell(n) - 1$ and the lower summation runs over all possible tuples of non-negative integers whose expansions to the base p concatenate to the expansion of n . We see that the sequence of polynomials $\{J_{\Lambda, n}; n \geq 0\}$ satisfies the defining relation (2.1) for the sequence $\{I_{\Lambda, n}; n \geq 0\}$. As we remarked earlier, such a sequence is unique. Therefore $J_{\Lambda, n} = I_{\Lambda, n}$ for every n , which finishes the proof of the lemma. \square

3. PROOF OF THEOREM 1

Define a new sequence of $h \times h$ matrices $\{\gamma_s; s \geq 0\}$ so that for every s

$$(3.1) \quad \alpha_s = \sum_{s_1 + \dots + s_r = s} \gamma_{s_1} \cdot \Phi^{s_1}(\gamma_{s_2}) \cdot \Phi^{s_1 + s_2}(\gamma_{s_3}) \cdot \dots \cdot \Phi^{\sum_{j=1}^{r-1} s_j}(\gamma_{s_r}),$$

where the summation runs over all ordered partitions of s into a sum of non-negative integers:

$$\sum_{s_1 + \dots + s_r = s} = \sum_{r=1}^s \sum_{\substack{(s_1, \dots, s_r) \in \mathbb{Z}_{\geq 1}^r \\ s_1 + \dots + s_r = s}}.$$

Formula (3.1) defines γ_s recursively, since in the right-hand side we have γ_s plus the sum of products of various Frobenius images of matrices $\gamma_{s'}$ with $s' < s$.

Lemma 2. $\gamma_s \equiv 0 \pmod{p^{s-1}}$ for every $s \geq 1$.

Proof. During this proof, let's forget that matrices γ_s were already defined and consider

$$(\gamma_s)_{u,v} := \left[I_{\Lambda, p^{s-1}} \right]_{x^{p^s v} - u}.$$

If we show that they satisfy (3.1), the statement will follow from (ii) in Lemma 1. We have

$$(3.2) \quad \Lambda^{p^s - 1} = \sum_{s_1 + \dots + s_r = s} I_{\Lambda, p^{s_1-1}} \cdot \Phi^{s_1}(I_{\Lambda, p^{s_2-1}}) \cdot \Phi^{s_1 + s_2}(I_{\Lambda, p^{s_3-1}}) \cdot \dots \cdot \Phi^{\sum_{j=1}^{r-1} s_j}(I_{\Lambda, p^{s_r-1}}).$$

Let's consider one term in the sum corresponding to (s_1, \dots, s_r) . For $k = 0, 1, \dots, r-1$ let's denote

$$A_k = I_{\Lambda, p^{s_{k+1}-1}} \cdot \Phi^{s_{k+1}}(I_{\Lambda, p^{s_{k+2}-1}}) \cdot \dots \cdot \Phi^{\sum_{j=k+1}^{r-1} s_j}(I_{\Lambda, p^{s_r-1}}),$$

so that the term under consideration is A_0 and for each k we have $A_k = I_{\Lambda, p^{s_{k+1}-1}} \cdot \Phi^{s_{k+1}}(A_{k+1})$. Let $u, v \in J$. To compute the coefficient near $x^{p^s v - u}$ in $A_0 = I_{\Lambda, p^{s_1-1}} \cdot \Phi^{s_1}(A_1)$, we notice that $\text{supp}(I_{\Lambda, p^{s_1-1}}) \subseteq (p^{s_1} - 1)\text{Newt}(\Lambda)$ by (i) in Lemma 1 and $\text{supp}(\Phi^{s_1}(A_1)) \subseteq p^{s_1} \text{supp}(A_1) \subset p^{s_1} \mathbb{Z}^N$. Suppose $w \in \text{supp}(I_{\Lambda, p^{s_1-1}})$ and $\tau \in \text{supp}(A_1)$ are such that

$$(3.3) \quad w + p^{s_1} \tau = p^s v - u.$$

Since $w \in (p^{s_1} - 1)\text{Newt}(\Lambda)$ and $u \in \text{Newt}(\Lambda)^o$, we have that $w + u \in p^{s_1} \text{Newt}(\Lambda)^o$. Moreover, (3.3) implies that $w + u \in p^{s_1} \mathbb{Z}^N$, and therefore $\frac{1}{p^{s_1}}(w + u) \in \text{Newt}(\Lambda)^o \cap \mathbb{Z}^N = J$. On the other hand, for every $\mu \in J$ vectors

$$w = p^{s_1} \mu - u, \quad \tau = p^{s-s_1} v - \mu$$

satisfy (3.3). It follows that

$$\left[I_{\Lambda, p^{s_1}-1} \cdot \Phi^{s_1}(A_1) \right]_{x^{p^{s_1}v-u}} = \sum_{\mu \in J} [I_{\Lambda, p^{s_1}-1}]_{x^{p^{s_1}\mu-u}} \cdot \Phi^{s_1} \left([A_1]_{p^{s-s_1}v-\mu} \right),$$

where we recognize matrix multiplication in the right-hand side. We then proceed by splitting $A_1 = I_{\Lambda, p^{s_2}-1} \cdot \Phi^{s_2}(A_2)$, and so on. Finally we obtain that

$$\begin{aligned} & \left[I_{\Lambda, p^{s_1}-1} \cdot \Phi^{s_1} \left(I_{\Lambda, p^{s_2}-1} \right) \cdot \Phi^{s_1+s_2} \left(I_{\Lambda, p^{s_3}-1} \right) \cdot \dots \cdot \Phi^{\sum_{j=1}^{r-1} s_j} \left(I_{\Lambda, p^{s_r}-1} \right) \right]_{x^{p^s v-u}} \\ &= \left(\gamma_{s_1} \cdot \Phi^{s_1}(\gamma_{s_2}) \cdot \Phi^{s_1+s_2}(\gamma_{s_3}) \cdot \dots \cdot \Phi^{\sum_{j=1}^{r-1} s_j}(\gamma_{s_r}) \right)_{u,v}. \end{aligned}$$

Summation over all partitions $s_1 + \dots + s_r = s$ in (3.2) gives us (3.1). \square

Proof of Theorem 1. In (3.1) terms corresponding to partitions $s_1 + \dots + s_r = s$ containing at least one $s_i > 1$ vanish modulo p due to Lemma 2. The only partition without $s_i > 1$ is $1 + \dots + 1 = s$, and therefore

$$\alpha_s \equiv \gamma_1 \cdot \Phi(\gamma_1) \cdot \dots \cdot \Phi^{s-1}(\gamma_1) \pmod{p}.$$

Part (i) follows immediately since $\alpha_1 = \gamma_1$.

We will prove (ii) by induction on s . The case $s = 1$ follows from part (i). From (3.1) we have

$$\alpha_s = \gamma_1 \Phi(\alpha_{s-1}) + \gamma_2 \Phi^2(\alpha_{s-2}) + \dots + \gamma_{s-1} \Phi^{s-1}(\alpha_1) + \gamma_s$$

for every $s \geq 1$. Substituting these expressions into the two sides of the congruence that we want to prove we get

$$\begin{aligned} \alpha_{s+1} \Phi(\alpha_s)^{-1} &= \gamma_1 + \sum_{j=2}^{s+1} \gamma_j \Phi^j(\alpha_{s+1-j}) \Phi(\alpha_s)^{-1}, \\ \alpha_s \Phi(\alpha_{s-1})^{-1} &= \gamma_1 + \sum_{j=2}^s \gamma_j \Phi^j(\alpha_{s-j}) \Phi(\alpha_{s-1})^{-1}. \end{aligned}$$

Since we want to compare these two expressions modulo p^s and $\gamma_{s+1} \equiv 0 \pmod{p^s}$, the last term in the upper sum can be ignored. For every $j = 2, \dots, s$ we use inductional assumption as follows:

$$\begin{aligned} \alpha_s \Phi(\alpha_{s-1})^{-1} &\equiv \alpha_{s-1} \Phi(\alpha_{s-2})^{-1} \pmod{p^{s-1}} \\ \alpha_{s-1} \Phi(\alpha_{s-2})^{-1} &\equiv \alpha_{s-2} \Phi(\alpha_{s-3})^{-1} \pmod{p^{s-2}} \\ &\vdots \\ \alpha_{s+2-j} \Phi(\alpha_{s+1-j})^{-1} &\equiv \alpha_{s+1-j} \Phi(\alpha_{s-j})^{-1} \pmod{p^{s+1-j}} \end{aligned}$$

We then apply the respective power of Φ to each row and multiply these congruence out to get that modulo p^{s+1-j}

$$\begin{aligned} \alpha_s \Phi^{j-1}(\alpha_{s+1-j})^{-1} &= \alpha_s \Phi(\alpha_{s-1})^{-1} \Phi(\alpha_{s-1}) \Phi^2(\alpha_{s-2})^{-1} \dots \Phi^{j-1}(\alpha_{s+1-j})^{-1} \\ &\equiv \alpha_{s-1} \Phi(\alpha_{s-2})^{-1} \Phi(\alpha_{s-2}) \Phi^2(\alpha_{s-3})^{-1} \dots \Phi^{j-1}(\alpha_{s-j})^{-1} = \alpha_{s-1} \Phi^{j-1}(\alpha_{s-j})^{-1}. \end{aligned}$$

Since determinants of these matrices are non-zero modulo p , we can invert them to get

$$\Phi^{j-1}(\alpha_{s+1-j}) \alpha_s^{-1} \equiv \Phi^{j-1}(\alpha_{s-j}) \alpha_{s-1}^{-1} \pmod{p^{s+1-j}}.$$

Now we apply Φ and multiply by γ_j . Since $\gamma_j \equiv 0 \pmod{p^{j-1}}$ we get

$$\gamma_j \Phi^j(\alpha_{s+1-j}) \Phi(\alpha_s)^{-1} \equiv \gamma_j \Phi^j(\alpha_{s-j}) \Phi(\alpha_{s-1})^{-1} \pmod{p^s}.$$

Summation in j gives the desired result. \square

4. THE CASE OF A SMOOTH PROJECTIVE HYPERSURFACE

Let's assume for simplicity that $R = \mathbb{Z}$ and Φ is the identity transformation. Let $F \in \mathbb{Z}[X_0, \dots, X_N]$ be an absolutely irreducible homogeneous polynomial of degree $d > N$, such that the hypersurface

$$(4.1) \quad X : F(X_0, \dots, X_N) = 0$$

is smooth. In this case

$$\dim H^0(X, \Omega_{X/R}^{N-1}) = \binom{d-1}{N}$$

(see e.g. [6] for this computation) is equal to the number of internal integral points in the Newton polytope $\text{Newt}(F) \subset \mathbb{R}^{N+1}$. Indeed, for a generic polynomial F (that is, all monomials of degree d are

present with nonzero coefficients) $\text{Newt}(F)$ is the simplex in the hyperplane $\sum_{i=0}^N u_i = d$ with $N+1$ vertices of the form $(0, \dots, 0, d, 0, \dots, 0)$, and the set of integral internal points is given by

$$(4.2) \quad J = \{u = (u_0, \dots, u_N) \in \mathbb{Z}^{N+1} : u_i \geq 1 \quad \forall i, \sum_{i=0}^N u_i = d\}.$$

When X is smooth, one can show that we still have $\text{Newt}(F)^\circ \cap \mathbb{Z}^{N+1} = J$.

An explicit basis in $H^0(X, \Omega_{X/R}^{N-1})$ corresponding to the elements of the set J in (4.2) can be given as follows. Let $f(x_1, \dots, x_N) = F(1, x_1, \dots, x_N)$. W.l.o.g. we can assume that $\frac{\partial f}{\partial x_N} \not\equiv 0$ on X . Then the forms

$$(4.3) \quad \begin{aligned} \omega_u &= x_1^{u_1-1} \cdots x_N^{u_N-1} \frac{dx_1 \wedge \cdots \wedge x_{N-1}}{\frac{\partial f}{\partial x_N}(x_1, \dots, x_N)} \\ u &= (u_0, \dots, u_N) \in J \end{aligned}$$

constitute a basis for $H^0(X, \Omega_{X/R}^{N-1})$.

Let p be a prime and $\overline{F} \in \mathbb{F}_p[X_0, \dots, X_N]$ be the reduction of F modulo p , and suppose that

$$\overline{X} : \overline{F}(X_0, \dots, X_N) = 0$$

is again a smooth hypersurface over \mathbb{F}_p . It is claimed in [3, Corollary 1] that the matrix of the Cartier operator

$$C : H^0(\overline{X}, \Omega_{\overline{X}/\mathbb{F}_p}^{N-1}) \rightarrow H^0(\overline{X}, \Omega_{\overline{X}/\mathbb{F}_p}^{N-1})$$

in the basis corresponding to (4.3) is given by

$$\begin{aligned} (C)_{u,v \in J} &= \text{the coefficient of } X^{pv-u} \text{ in } \overline{F}(X)^{p-1} \\ &= \alpha_1 \mod p, \end{aligned}$$

where $\alpha_1 = \beta_{p-1}$ in the notation of Section 1 with $\Lambda = F$.

We see that α_1 is invertible as a matrix with \mathbb{Z}_p -entries if and only if the Cartier operator is invertible. If α_1 is invertible, then $\det(\alpha_1) \not\equiv 0 \mod p$ and $\det(\alpha_s) \equiv \det(\alpha_1)^s \not\equiv 0 \mod p$, so all α_s are invertible as well.

5. APPLICATION OF ATKIN AND SWINNERTON-DYER TYPE CONGRUENCES

In this section we combine Theorem 1 with the main result of [2]. Here again $R = \mathbb{Z}$ and Φ is trivial. Let $G(X_0, \dots, X_N)$ be a polynomial with integral coefficients, homogeneous of degree $2d$, and $d > N$. Let X be the double covering of \mathbb{P}^N defined by the equation $W^2 = G(X_0, \dots, X_N)$. Let

$$\Lambda(W, X_0, \dots, X_N) = W^2 - G(X_0, \dots, X_N).$$

Let J be the set from (4.2), that is

$$J = \left\{ u = (u_0, \dots, u_N) \in \mathbb{Z}^{N+1} : u_i \geq 1 \quad \forall i, \sum_{i=0}^N u_i = d \right\}.$$

For a generic G (that is, every monomial of degree $2d$ is present with a nonzero coefficient), we claim that $\text{Newt}(\Lambda)^\circ \cap \mathbb{Z}^{N+2} = \{(1, u) : u \in J\}$. Indeed, $\text{Newt}(G)$ is the simplex in the hyperplane $\sum_{i=0}^N u_i = 2d$ with $N+1$ vertices of the form $(0, \dots, 0, 2d, 0, \dots, 0)$, and

$$\text{Newt}(G)^0 = \{u \in \mathbb{R}^{N+1} : u_i > 0 \quad \forall i, \sum_{i=0}^N u_i = 2d\}.$$

$\text{Newt}(\Lambda)$ is the convex hull of $(2, 0, \dots, 0)$ and $0 \times \text{Newt}(G)$ in \mathbb{R}^{N+2} , so our claim follows.

When X is smooth, it is shown in [1, Appendix A4] that $\dim H^0(X, \Omega_{X/R}^N) = \binom{d-1}{N}$, and an explicit basis of global N -forms indexed by the elements of J is constructed.

Let $h = \#J = \binom{d-1}{N}$. We will assume further on that $\text{Newt}(\Lambda)^\circ \cap \mathbb{Z}^{N+2} = \{(1, u) : u \in J\}$. We consider $h \times h$ matrices from Section 1:

$$(\beta_n)_{u,v \in J} = \text{the coefficient of } W^n X^{(n+1)v-u} \text{ in } \Lambda^n = \begin{cases} 0, & n \text{ odd,} \\ (-1)^{\frac{n}{2}} \binom{n}{n/2} \cdot \delta_n, & n \text{ even,} \end{cases}$$

where

$$(\delta_n)_{u,v \in J} = \text{the coefficient of } X^{(n+1)v-u} \text{ in } G^{\frac{n}{2}}.$$

Let's now fix a prime p and consider the subsequence of matrices $\alpha_s = \beta_{p^s-1}$, $s \geq 0$. Assuming that $\det(\alpha_1) \neq 0 \pmod{p}$, we have that all α_s are invertible over \mathbb{Z}_p by (i) of Theorem 1 and by (ii) there exists the limiting $h \times h$ matrix

$$\alpha := \lim_{s \rightarrow \infty} \alpha_s \alpha_{s-1}^{-1}$$

with entries in \mathbb{Z}_p .

Let $\overline{X} = X \times_{\text{Spec}(\mathbb{Z})} \text{Spec}(\mathbb{F}_p)$ be the fibre of X at p , and suppose that there exists a smooth projective variety \overline{Y} over \mathbb{F}_p and a morphism $\pi : \overline{Y} \rightarrow \overline{X}$ such that $\pi_* \mathcal{O}_{\overline{Y}} = \mathcal{O}_{\overline{X}}$ and $R^i \pi_* \mathcal{O}_{\overline{Y}} = 0$ for $i \geq 1$. Consider the (reciprocal) characteristic polynomial of the p th power Frobenius Frob_p acting on the middle crystalline cohomology of \overline{Y}

$$\det(1 - T \cdot \text{Frob}_p | H_{\text{cris}}^N(\overline{Y}) \otimes \mathbb{Q}) = 1 + a_1 T + \dots + a_k T^k \in \mathbb{Z}[T].$$

Let n be a positive integer and ν be the maximal integer such that $p^\nu | n$. By [2, Theorem 0.1], if $\nu \geq h$ then

$$(5.1) \quad \delta_{n-1} + a_1 \delta_{\frac{n}{p}-1} + \dots + a_k \delta_{\frac{n}{p^k}-1} \equiv 0 \pmod{p^{\nu-h+1}},$$

where we assume that $\delta_n = 0$ for $n \notin 2\mathbb{N}$.

Corollary 1. *When $\det(\alpha_1) \neq 0 \pmod{p}$, the matrix $\alpha = \lim_{s \rightarrow \infty} \alpha_s \alpha_{s-1}^{-1}$ satisfies*

$$\alpha^k + a_1 \alpha^{k-1} + \dots + a_{k-1} \alpha + a_k = 0.$$

Proof. The sequence

$$b_n = \begin{cases} 0, & n \text{ odd}, \\ (-1)^{\frac{n}{2}} \binom{n}{n/2}, & n \text{ even} \end{cases}$$

is the sequence of constant terms of the polynomial $\Lambda(x) = x - \frac{1}{x}$, to which Theorem 1 is applicable. It follows that

$$\frac{b_{p^{s+1}-1}}{b_{p^s-1}} \equiv \frac{b_{p^s-1}}{b_{p^{s-1}-1}} \pmod{p^s}$$

for every $s \geq 1$. One can show, using for instance p -adic gamma function, that actually

$$\frac{b_{p^s-1}}{b_{p^{s-1}-1}} \equiv 1 \pmod{p^s},$$

and therefore

$$\alpha_s \cdot \alpha_{s-1}^{-1} \equiv \delta_{p^s-1} \cdot \delta_{p^{s-1}-1}^{-1} \pmod{p^s}$$

and

$$\alpha = \lim_{s \rightarrow \infty} \delta_{p^s-1} \delta_{p^{s-1}-1}^{-1}.$$

The result now follows from Stienstra's congruences (5.1). \square

We see that eigenvalues of α are also eigenvalues of the p th power Frobenius Frob_p . Since $\det(\alpha) \equiv \det(\alpha_1) \pmod{p}$ and $\det(\alpha_1) \neq 0 \pmod{p}$, the eigenvalues of α are p -adic units.

6. AN EXAMPLE

Consider the hyperelliptic curve

$$y^2 = x^5 + 2x^2 + x + 1.$$

Stienstra's matrices here will have size 2×2 :

$$\beta_n = \text{the coefficients of } \begin{pmatrix} x^n y^n & x^{2n+1} y^n \\ x^{n-1} y^n & x^{2n} y^n \end{pmatrix} \text{ in } (y^2 - x^5 - 2x^2 - x - 1)^n.$$

For example, with $p = 11$ we have

| s | 0 | 1 | 2 | 3 |
|--|--|--|---|-----|
| $\alpha_s = \beta_{p^s-1}$ | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} -81144 & -1260 \\ -81900 & -1260 \end{pmatrix}$ | ... | ... |
| $\text{tr}(\alpha_s \cdot \alpha_{s-1}^{-1}) \pmod{p^s}$ | $8 + O(11)$ | $8 + 11 + O(11^2)$ | $8 + 11 + 11^2 + O(11^3)$ | |
| $\det(\alpha_s \cdot \alpha_{s-1}^{-1}) \pmod{p^s}$ | $7 + O(11)$ | $7 + 6 \cdot 11 + O(11^2)$ | $7 + 6 \cdot 11 + 3 \cdot 11^2 + O(11^3)$ | |

Using Kedlaya's algorithm we computed the reciprocal characteristic polynomial of the Frobenius on the first crystalline cohomology of the curve:

$$\begin{aligned} \det\left(1 - T \cdot \text{Frob}_{11} \mid H_{\text{cris}}^1(C)\right) &= 1 + 3T + 18T^2 + 3 \cdot 11T^3 + 11^2T^4 \\ &= (1 + 4T + 11T^2)(1 - T + 11T^2) \end{aligned}$$

The eigenvalues of the Frobenius are

$$\lambda_{1,2} = -2 \pm \sqrt{-7}, \quad \lambda_{3,4} = \frac{1 \pm \sqrt{-43}}{2}.$$

Both -7 and -43 are squares modulo 11 , and 11 -adic unit eigenvalues are

$$\begin{aligned} \lambda_1 &= 7 + 2 \cdot 11 + 2 \cdot 11^2 + O(11^3) \\ \lambda_3 &= 1 + 10 \cdot 11 + 9 \cdot 11^2 + O(11^3) \end{aligned}$$

We see that in the above table traces and determinants converge to

$$\begin{aligned} \lambda_1 + \lambda_3 &= 8 + 11 + 11^2 + O(11^3) \\ \lambda_1 \cdot \lambda_3 &= 7 + 6 \cdot 11 + 3 \cdot 11^2 + O(11^3) \end{aligned}$$

respectively.

We hope that on practice our method can be used in the other direction, in order to compute Frobenius data modulo a given power of p using coefficients of powers of the equation of the hypersurface.

REFERENCES

- [1] J. Stienstra, *Formal group laws arising from algebraic varieties*, American Journal of Mathematics, 109, no. 5 (1987), pp. 907-925
- [2] J. Stienstra, *Formal groups and congruences for L-functions*, American Journal of Mathematics, 109, no. 6 (1987), pp. 1111-1127
- [3] L. Miller, *The Hasse-Witt-matrix of special projective varieties*, Pacific Journ. Math., Vol. 43 (1972), no. 2, pp.443-455
- [4] N. Katz, *Internal reconstruction of unit-root F-crystals via expansion-coefficients*, Annales scientifiques de l'É.N.S. 4e série, tome 18, no. 2(1985), pp. 245-285
- [5] A. Mellit, M. Vlasenko, *Dwork congruences for the constant terms of powers of a Laurent polynomial*, 2013, arXiv:1306.5811 [math.NT]
- [6] Liviu I. Nicolaescu, *Hodge numbers of complete intersections*, <http://www3.nd.edu/~lnicolae/hodgeint.pdf>